

(11)特許出願公開番号

特開平10-70576

(43)公開日 平成10年(1998)3月10日

(51)Int.Cl. <sup>6</sup>	識別記号	序内整理番号	F I	技術表示箇所
H 0 4 L 12/66		9744-5K	H 0 4 L 11/20	B
G 0 6 F 13/00	3 5 3		G 0 6 F 13/00	3 5 3 T
	3 5 7			3 5 7 Z
H 0 4 L 12/24		9744-5K	H 0 4 L 11/08	
12/26				

審査請求 未請求 請求項の数3 O.L (全 7 頁)

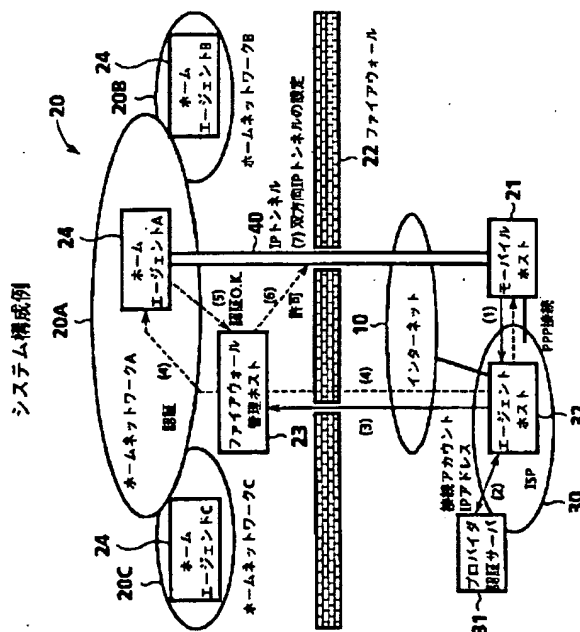
(21)出願番号	特願平8-227969	(71)出願人	000001214 国際電信電話株式会社 東京都新宿区西新宿2丁目3番2号
(22)出願日	平成8年(1996)8月29日	(72)発明者	窪田 歩 東京都新宿区西新宿二丁目3番2号 国際 電信電話株式会社内
		(72)発明者	片岸 一起 東京都新宿区西新宿二丁目3番2号 国際 電信電話株式会社内
		(72)発明者	浅見 徹 東京都新宿区西新宿二丁目3番2号 国際 電信電話株式会社内
		(74)代理人	弁理士 光石 俊郎 (外2名)

(54) 【発明の名称】 ファイアウォール動的制御方法

(57) 【要約】

【課題】 インターネットサービスプロバイダ（ISP）にダイヤルアップ接続中の移動端末及びそのユーザに対してファイアウォールのフィルタ設定を適切に行い、更に、ホームネットワーク資源へのアクセスを適切に許可できること。

【解決手段】 I S P 3 0 にダイヤルアップにより接続中の端末21がインターネット10を経由してファイアウォール22内の内部ネットワーク20にアクセスする際に、I S P 3 0 から端末21のユーザ情報を送り、このユーザ情報を基に端末21が内部ネットワーク20から移動した移動端末であるか否かを判断し、移動端末である場合に、同端末21と内部ネットワーク20との通信を許可するようにファイアウォール22のフィルタを設定し、更に、同端末21と内部ネットワーク20との通信をI P トンネル40により行う。



## 【特許請求の範囲】

【請求項1】 インターネットサービスプロバイダにダイヤルアップにより接続中の端末がインターネットを経由してファイアウォール内の内部ネットワークにアクセスする際に、前記インターネットサービスプロバイダから前記内部ネットワークに前記端末のユーザ情報を送ること、前記内部ネットワークはこのユーザ情報を基に前記端末が同内部ネットワークから移動した移動端末か否かを判断すること、前記端末が移動端末である場合に同

端末と内部ネットワークとの通信を許可するようにファイアウォールのフィルタを設定することを特徴とするファイアウォール動的制御方法。

【請求項2】 前記フィルタの設定後、前記端末と内部ネットワークとの通信をIPトンネルにより行うことを特徴とする請求項1に記載のファイアウォール動的制御方法。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はファイアウォールを動的に制御する方法に関する。

【0002】

【従来の技術】社内ネットワークをインターネットに接続している場合、インターネットからの不正アクセスを防ぐ必要がある。但し、外部ネットワークと内部ネットワーク間の通信を完全に遮断すると、ユーザが外出先からインターネット経由でホームネットワークにアクセスしようとしても、これが不可能になる。

【0003】（ファイアウォールとフィルタ処理）そのため、インターネットを経由した外部からの通信を選択的に通過させるファイアウォール（防火壁）の構築が必須となっている。

【0004】従来、ファイアウォールでは、内部ネットワークと外部ネットワークの間で通信されるデータパケットの内、予め許可されているパケットのみを通し、それ以外のパケットを遮断するというフィルタ処理が行われている。

【0005】フィルタの設定は、通常、送信元端末のIP（Internet Protocol:インターネット通信規約）アドレス、送信先端末のIPアドレス、使用プロトコルの種類、及び、ポート番号等を指定することにより行われる。例えば、外部の特定IPアドレスから内部の任意ホスト（端末）へのTCP（Transmission Control Proto

col:伝送制御通信規約）プロトコルによる通信を行う場合、或るポート番号（例えば110）を使用しているものに限り許可するといった設定がなされる。

【0006】なお、ポート番号とは、TCP、UDP（User Datagram Protocol）において上位層のプロセスを特定するために使用する識別子である。

【0007】しかし、ノート型パソコン等の携帯型コンピュータをユーザが持ち歩き、移動先でインターネットサービスプロバイダ（ISP（Internet Service Provider）と略記する）経由のダイヤルアップ接続（PPP接続とも称される）によりインターネットに接続して、ホームネットワークへのアクセスを行う場合は、適切なフィルタ処理を行うことが難しい。

【0008】これは、インターネットの通信に用いられるIPアドレスは4バイトの数値で表されるが、その上位桁部分は端末が接続されているネットワークを表し、下位部分がそのネットワーク内での当該端末の識別番号になっているためである。つまり、ホームネットワークから移動した端末（モバイルホスト：MH（Mobile host）と略記する）でダイヤルアップ接続を行う場合は、その移動端末に割り当てられるIPアドレスが接続の度に変わり、ホームネットワークでのIPアドレスをそのまま使用して通信を行うことができない。このようにダイヤルアップ接続の場合は移動端末のIPアドレスが一定しないことから、ファイアウォールにおいてデータパケットの送信元端末のIPアドレス及び送信先端末のIPアドレスを特定してフィルタを設定することが不可能になる。

【0009】しかも、仮にファイアウォールのフィルタ設定を適切に行い、権限を持つ移動端末及びそのユーザによる外部から内部へのアクセスのみを許可することが可能になったとしても、同ユーザが普段ホームネットワークでアクセスしている共有ディスク、社内データベース、及び、WWW（World Wide Webの略）の社内向けページといった各種内部ネットワーク資源の利用が可能になるとは限らない。

【0010】何故ならば、これら内部ネットワーク資源には個別にアクセス制限が行われている場合があり、その際、クライアント端末のIPアドレスに基づいてアクセスの許可及び不許可を決める場合が多いからである。

【0011】（モバイルIP）次に、現在標準化が進められているモバイルIP（Mobile-IP）を、図3を参照して説明する。モバイルIPとは、端末が何処に移動してインターネットに接続しても、他の端末が当該移動端末に対して、常に同じIPアドレスを用いて通信を行うことを可能にする技術である。但し、現状のモバイルIPは仕様上、ファイアウォールを持つネットワークには未対応である。

【0012】図3において、100はインターネット、200は移動端末201のホームネットワーク、202

10

20

30

40

50

はホームネットワーク200上のホームエージェント（HA（Home Agent）と略記する）、203はルータ、300はISP、400は他のネットワーク、401は他のネットワーク400上の端末をそれぞれ示す。

【0013】ここでは、移動端末201が通常接続されているホームネットワーク200のIPアドレスを[133.128.8.0]とし、同ホームネットワーク200における移動端末201のIPアドレスを[133.128.8.81]とし、ホームエージェント202のIPアドレスを[133.128.8.100]とし、移動端末201がISP300にダイヤルアップ接続した時に割り当てられるIPアドレスを[130.54.20.199]としている。

【0014】一般に、或るネットワーク400の端末401から端末201宛にパケットが送出されると、図3中に符号501で示す経路のように、端末201が通常接続されているホームネットワーク200に配送される。そのため、端末201が別のネットワーク例えばISP300に移動している場合には、パケットを移動先のネットワーク300に転送する必要がある。

【0015】この転送を行うため、モバイルIPでは、移動元のネットワークと移動先のネットワークにそれぞれエージェントホストが設置される。移動元ネットワークに設置されるエージェントホストはホームエージェントと呼ばれる。移動先のネットワークに設置されるエージェントホストはフォーリンエージェント（FA（Foreign Agent）と略記する）と呼ばれる。移動端末自身がフォーリンエージェントの役割を果たすことも可能である。図3では、移動端末201がフォーリンエージェントの機能を有するものとしている。

【0016】端末201がホームネットワーク200から移動してISP300にダイヤルアップ接続301を行うと、ISP300から一時的なIPアドレス[130.54.20.199]が割り当てられる。

【0017】そこで、移動端末201はこのIPアドレスと、通常接続しているホームネットワーク200におけるIPアドレス[133.128.8.81]とをISP300及びインターネット100を経由してホームネットワーク200のホームエージェント202に通知しておく。これにより、ホームエージェント202はIPアドレス[133.128.8.81]を持つ端末201が移動中であり、それが一時的に取得したIPアドレスが[130.54.20.199]であることを知るので、データベースに記録しておく。

【0018】そして、或るネットワーク400内の端末401から通常のIPアドレス[133.128.8.81]を用いて端末201宛のパケットが届くと、端末201の代わりにホームエージェント202が受け取る（経路502参照）。ホームエージェント202は、端末401から移動端末201宛の前記パケットを、一時的に取得したIPアドレス[130.54.20.199]向けのパケットに埋め込み、インターネット100及びISP300を経由して

移動端末201に転送する（経路503参照）。移動端末201は受け取ったパケットから元のパケットを取り出し、必要に応じて送信元の端末401宛にISP300及びインターネット100を経由してパケットを送る（経路504参照）。

【0019】上述の如く、モバイルIPによれば、端末401からは移動中の端末201に、その通常のIPアドレス[133.128.8.81]を用いてパケットを送ることができる。

10 【0020】しかし、移動端末201とホームエージェント202との間では、一時的に取得したIPアドレス[130.54.20.199]を用いて通信が行われる。

【0021】つまり、現状のモバイルIPでは、移動端末201が送出するパケットには一時的に取得したIPアドレスを用いて何らの処理も加えないため、通常通りルーティングされる。従って、前述したフィルタ処理によるファイアウォールの設定では、移動端末201とホームエージェント202間の通信のみを許可するので、移動端末201がホームエージェント202以外のホームネットワーク200内の内部ホスト（端末）と通信を行うことができない。これは、各種内部ネットワーク資源への移動端末201のアクセスが制限されることを意味する。

20 【0022】

【発明が解決しようとする課題】本発明は上記問題点を鑑み、インターネットサービスプロバイダ（ISP）にダイヤルアップ接続中の移動端末及びそのユーザに対して適切なフィルタ設定を行うことができるファイアウォール動的制御方法、並びに、同端末及びユーザが外部からホームネットワーク資源へアクセスすることを適切に許可することができるファイアウォール動的制御方法を提供することを目的とする。

30 【0023】

【課題を解決するための手段】まず本発明では、インターネットサービスプロバイダからユーザ情報を得ることにより、このユーザ情報を基にフィルタの設定を適切に行うことを可能にする。また本発明では、このフィルタ設定に、現在標準化が進められているモバイルIPの技術を改良して組み合わせることにより、ホームネットワーク資源へのアクセス制限の問題を解決する。

40 【0024】即ち、本発明のファイアウォール動的制御方法は、インターネットサービスプロバイダにダイヤルアップにより接続中の端末がインターネットを経由してファイアウォール内の内部ネットワークにアクセスする際に、前記インターネットサービスプロバイダから前記内部ネットワークに前記端末のユーザ情報を送ること、前記内部ネットワークはこのユーザ情報を基に前記端末が同内部ネットワークから移動した移動端末か否かを判断すること、前記端末が移動端末である場合に同端末と内部ネットワークとの通信を許可するようにファイアウ

ォールのフィルタを設定することを特徴とする。

【0025】また、本発明のファイアウォール動的制御方法は、前記フィルタの設定後、端末と内部ネットワークとの通信をIPトンネルにより行うことを特徴とし、或いは、更に前記端末のユーザ情報の送信をインターネットサービスプロバイダに設けたエージェントホストと内部ネットワークに設けたファイアウォールのフィルタの設定を行うファイアウォール管理用ホストとの間で行うこと、前記IPトンネルによる通信を前記端末と内部ネットワークに設けたホームエージェントとの間で行うことを特徴とする。

【0026】

【発明の実施の形態】以下、図1と図2を参照して本発明の実施の形態を説明する。図1は本発明のファイアウォール動的制御方法を適用したシステム構成例を示す図、図2はファイアウォールに対応したモバイルIPの説明図である。

【0027】図1において、10はインターネット、20は複数のホームネットワーク20A、20B、20Cを有する或る内部ネットワーク、21は通常内部ネットワーク20に接続されている移動端末、22はファイアウォール、23はファイアウォール管理用ホスト、24は各ホームネットワーク20A、20B、20Cに設けたホームエージェント、30はISP（インターネットサービスプロバイダ）、31はISP30のプロバイダ認証サーバ、32はISP30のエージェントホストをそれぞれ示す。

【0028】移動端末21はモバイルIP用のフォーリンエージェント機能を有し、移動先でISP30にダイヤルアップ接続し、インターネット10を介して内部ネットワーク20に接続しようとしているものとする。

【0029】本実施例では、以下のようにして、ISP30から得るユーザ情報を基にファイアウォールの制御を行う機構と、ファイアウォール22に対応させたモバイルIPの機構を用意している。

【0030】（ファイアウォールの動的制御機構）まず、図1を参照して、ISP30から得るユーザ情報を基にファイアウォール22の制御を行うファイアウォールの動的制御機構の構成を説明する。

【0031】移動端末21のユーザがISP30へダイヤルアップ接続する際には、ユーザアカウント（ID）とパスワードを入力する。ISP30では、ユーザの入力データが適正か否かをプロバイダ認証サーバ31により判定し、適正な場合のみ、移動端末21にIPアドレスを割り当ててインターネット100に接続する。そのため、ISP30側では、ユーザアカウントとパスワードを基にどのようなユーザが現在ダイヤルアップで接続中であるか、また、その移動端末21にはどのIPアドレスを割り当てたかというユーザ情報を常に把握できている。

【0032】そのため、このユーザ情報をISP30側から内部ネットワーク20が取得して、現在どのユーザがどのIPアドレスを使っているかが判れば、前述のフィルタの設定を適切に行うことが可能になる。これにより、内部ネットワーク20へのアクセスが予め許されたユーザからの通信のみを許可し、内部へのアクセス権限のないユーザからのアクセスを排除することができる。

【0033】そこで、図1に示すように、ファイアウォール管理用ホスト23を内部ネットワーク20に設けることにより、フィルタの追加・削除を行う機構を用意する。また、ISP30側にエージェントホスト32を設け、このエージェントホスト32とファイアウォール管理用ホスト23間の通信のみを許可しておく。この通信には、ファイアウォール管理用ホスト23もエージェントホスト32も固定したIPアドレスを用いることができるので、ファイアウォール用フィルタ設定に何の障害もない。具体的には、下記（1）～（7）の手順が採られる。なお、下記手順（n）は図1中の同記号（n）に対応している。

【0034】（1）外部から内部へのアクセスを行う移動端末21は、ISP30のエージェントホスト32経由で、内部ネットワーク20とのコネクション確立要求を行う。

（2）エージェントホスト32は、移動端末21のIPアドレスとダイヤルアップ接続時のアカウントを調べる。

（3）エージェントホスト32は、移動端末21がファイアウォール22内部へのアクセスを許可された特定アカウントで接続されている場合のみ、移動端末21からのメッセージをファイアウォール管理用ホスト23に中継する。

（4）モバイルIPでは移動端末とホームエージェントとの間でエンド・ツー・エンドの認証を行うことになっているので、ファイアウォール管理用ホスト23を通して移動端末21とホームエージェント24との間でエンド・ツー・エンドの認証を行う。

（5）この認証が成功すれば、その旨のメッセージをホームエージェント24がファイアウォール管理用ホスト23に送る。

（6）この結果、ファイアウォール管理用ホスト23は移動端末21とホームエージェント24間の通信を通過させるように、ファイアウォール22のフィルタ設定を変更する。

（7）ファイアウォール22の設定を変更して移動端末21とホームエージェント24間の通信を可能にした時点で、ファイアウォール管理用ホスト23はその旨をホームエージェント24へ通知するとともに、エージェントホスト32経由で移動端末21へも通知する。この通知を受けて、ホームエージェント24が移動端末21へのIPトンネルを設定し、また、移動端末21がホーム

エージェント24へのIPトンネルを設定することで、双方向IPトンネル40が設定される。

【0035】このIPトンネル40を用いて、移動端末21が内部ネットワーク20の各端末との通信を行う。ただし、移動端末21はコネクションの継続のためのメッセージをファイアウォール管理用ホスト23へ定期的に送るものとし、継続要求の途絶えたホスト向けのフィルタ設定は、ファイアウォール管理用ホスト23が自動的に削除するものとしている。

【0036】以上により、必要な期間のみ、始点と終点が明確に限定された通信のみを許可するファイアウォール22の設定が可能である。また、双方向IPトンネル40の設定が可能である。

【0037】前述の如く、現在標準化が進められているモバイルIPの仕様は、ファイアウォール22の有るネットワーク20には対応していない。そのため、モバイルIPをファイアウォール22に対応するように、下記の如く改良し、前述のフィルタの設定法と組み合わせて用いる。

【0038】（ファイアウォール対応モバイルIP）図2を参照して、モバイルIPとファイアウォール動的制御との組み合わせ方について説明する。

【0039】移動端末21からファイアウォール22内部の端末25へ送信するパケットは、図2中の経路52のように、ホームエージェント24宛のパケットに埋め込んで送出す。ホームエージェント24は、受け取ったパケットから元のパケットを取り出す。そして、ホームエージェント24は図2中の経路53のように、元のパケットを再びネットワーク20に送出することで、本来の宛て先である内部端末25に配送する。図2中の符号26はルータを示す。なお、ネットワーク20内に居る場合には、移動端末21は経路51で端末25と通信する。

【0040】このように、移動端末21とホームエージェント24間で双方向にカプセル化（トンネリング）を行うことにより、ネットワーク20内で個別にアクセス制限が行われている場合でも、移動端末21がネットワ

ーク20に通常接続されている場合のIPアドレスに基づいてアクセスを許可できるから、移動端末21とファイアウォール22内部の端末25との通信が可能である。

【0041】

【発明の効果】本発明によれば、ダイアルアップ接続中の特定ユーザからの通信のみを通過させるようなファイアウォールの設定が、ISPとの連携により可能である。

【0042】また、本発明によれば、モバイルIPを改良して組み合わせることにより、外部からでも、内部ネットワークに接続している時と全く同じ権限で、普段利用している内部ネットワーク資源へアクセスすることが可能である。

【図面の簡単な説明】

【図1】本発明のファイアウォール動的制御方法を適用したシステム構成例を示す図。

【図2】ファイアウォールに対応したモバイルIPの説明図。

【図3】ファイアウォールに未対応の従来のモバイルIPの説明図。

【符号の説明】

10 インターネット

20 内部ネットワーク

20A、20B、20C ホームネットワーク

21 フォーリンエージェント機能を有する移動端末

22 ファイアウォール

23 ファイアウォール管理用ホスト

24 ホームエージェント

25 内部端末

26 ルータ

30 ISP（インターネットサービスプロバイダ）

31 プロバイダ認証サーバ

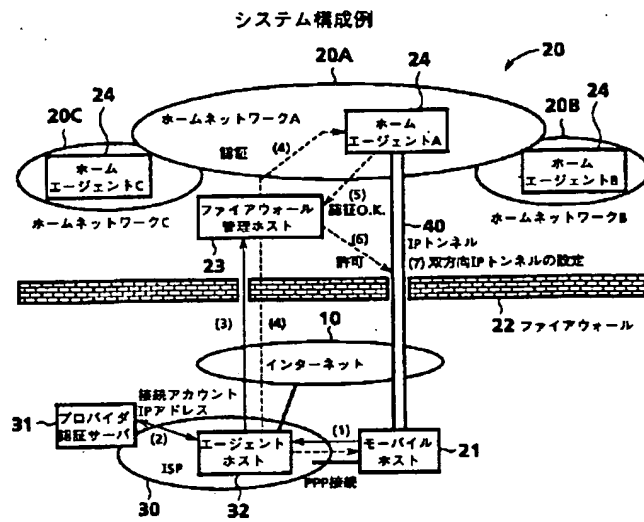
32 エージェントホスト

40 双方向IPトンネル

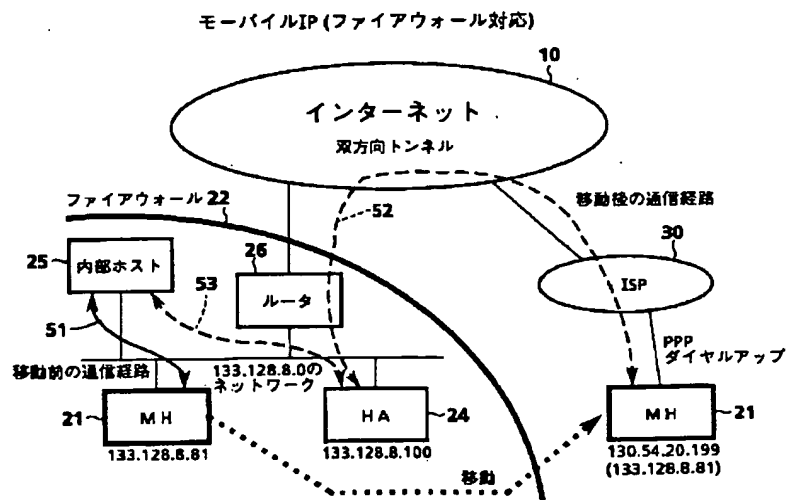
51 移動前の通信経路

52、53 移動後の通信経路

【図1】



【図2】



【図3】

